A Novel Approach of Secure Routing Protocol for Mobile Ad Hoc Network

Thesis submitted in partial fulfilment of the requirements for the degree of

Master of Technology

in

Computer Science and Engineering

(*Specialization: Information Security*)

by

Imran Hossain Faruk

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela – 769 008, India

A Novel Approach of Secure Routing Protocol for Mobile Ad Hoc Network

Dissertation submitted in

June 2013

to the department of

Computer Science and Engineering

of

National Institute of Technology Rourkela

in partial fulfillment of the requirements

for the degree of

Master of Technology

by

Imran Hossain Faruk

(Roll 211CS2069)

under the supervision of

Prof. Pabitra Mohan Khilar

Department of Computer Science and Engineering

National Institute of Technology Rourkela

Rourkela – 769 008, India

Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, India. www.nitrkl.ac.in

June 3, 2013

Certificate

This is to certify that the work in the thesis entitled **A Novel Approach of Secure Routing Protocol for Mobile Ad Hoc Network** by **Imran Hossain Faruk**, bearing roll number **211CS2069**, is a record of an original research work carried out by him under my supervision and guidance in partial fulfilment of the requirements for the award of the degree of **Master of Technology** in **Computer Science and Engineering**. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Prof. Pabitra Mohan Khilar
Dept. of Computer Science and Engineering
National Institute of Technology, Rourkela

Acknowledgment

First of all I would like to thank, my Parents, without their moral support and blessings I wouldn't have been writing this "thesis".

I would like to express my deep sense of respect and gratitude towards my supervisor Prof. Pabitra Mohan Khilar, who has been the guiding force behind this work. Without his unconditional support it wouldn't have been possible. As my supervisor, he has constantly encouraged me to remain focused on achieving my goal. I want to thank him for giving me the opportunity to work under him. His invaluable advice and assistance helped me to complete this thesis. I consider it my good fortune to have got an opportunity to work with such a wonderful person.

I am very much indebted to Prof. Ashok Kumar Turuk, Head-CSE, for his continuous encouragement and support. He is always ready to help with a smile. I am also thankful to all the professors of the department for their support. I am really thankful to all my friends. My sincere thanks to everyone who has provided me with kind words, a welcome ear, new ideas, useful criticism, or their invaluable time, I am truly indebted.

I must acknowledge the academic resources that I have got from NIT Rourkela. I would like to thank administrative and technical members of the Department who have been kind enough to advise and help in their respective roles.

Last,but not the least, I would like to dedicate this thesis to my family, for their love, patience, and understanding.

Imran Hossain Faruk

Abstract

Security in mobile ad hoc network is a grand challenge problem nowadays. The security issues in MANET are mostly concentrated in two parts, establishing secure route and securely data transmission. The main security threat in MANET are integrity, non-repudiation and privacy. To combat with these security threats, many secure routing protocols has been designed to reduce the security threats in MANET. Most of the secure routing protocol available in the literature are based on certification authority or key distribution center, which leads to needs of central authority. In this thesis, we have proposed a secure routing protocol called "A Novel Approach of Secure Routing Protocol (NASRP)" to enhance the security levels in the routing protocol to prevent the network against active and passive attacks without the presence of central authority. A peer review process has been introduced to check the integrity and non-repudiation of the routing packets and key exchange packets. In the first step each node will exchange keys with their neighbours, in the second step routing packet delivery is done by the peer review process and in the final stage data delivery is done by encryption/decryption mechanism using session key.

***Keywords*:** Secure Routing Protocol, Dynamic Source Routing, NASRP, Public Key Exchange, Certification Authority, Key-Distribution Center , Ad Hoc on Demand Distance Vector, Secret Key, Routing Attacks, Peer Review Process.

Contents

Certificate ii

Acknowledgement iii

Abstract iv

List of Figures viii

List of Tables ix

List of Abbreviations x

1 Introduction 1

1.1 Introduction 1

1.2 Motivation 2

1.3 Objective 2

1.4 Thesis Organization 3

1.5 Summary 3

2 Background Concepts 4

2.1 Introduction 4

2.2 Mobile Ad Hoc Networks 5

2.2.1 Application of Mobile Ad Hoc Network 6

2.2.2 Characteristics, Complexities and Design Constraints 8

2.3 Security Issues in Mobile Ad Hoc Networks 9
2.3.1 Passive Attacks 9
2.3.2 Active Attacks 9
2.4 Different type of attacks on ad hoc network routing protocols 12
2.5 Routing Protocol 13
2.5.1 Ad Hoc on Demand Distance Vector (AODV) Routing Protocol 13
2.5.2 Dynamic Source Routing (DSR) Protocol 14
2.6 Summary 14

3 Literature Survey **15**
3.1 Introduction 15
3.2 Literature Survey 15
3.3 Summary 18

4 Proposed Scheme 1 **19**
4.1 Introduction 19
4.2 Proposed CSRP Algorithm 20
4.2.1 Description 20
4.2.2 Design 20
4.3 CSRP Architecture 23
4.4 Summary 24

5 Proposed Scheme 2 **25**
5.1 Introduction 25
5.2 A Novel Approach of Secure Routing Protocol 26
5.2.1 Preliminaries 26
5.2.2 Description 26
5.2.3 Design 27
5.2.4 Architecture 31
5.3 Summary 35

6 Proposed Model Analysis **36**

6.1 Introduction 36

6.2 Analysis 37

6.2.1 Key Exchange between Neighbours 37

6.2.2 Analysis of RREQ packets 39

6.2.3 Analysis of RREP packets 40

6.2.4 Analysis of Data packet Transmission 41

6.3 Summary 42

7 Comparison **43**

7.1 Introduction 43

7.2 Comparison with other secure routing protocols 43

7.3 Average Transmission Delay Comparison 44

7.4 Summary 45

8 Conclusion and Future Works **46**

8.1 Conclusion 46

8.2 Future Work 46

Bibliography **47**

List of Figures

2.1 A Typical Mobile Ad Hoc Network 6

4.1 CSRP architecture with secret keys 23
4.2 Session Key establishment 23
4.3 Session Key established between the nodes 24
4.4 Flooding of RREQ to D and RREP from D to S 24
4.5 Data delivery by encryption and decryption using session key 24

5.1 RREQ Packet format of AODV, DSR and NASRP 27
5.2 A MANET network 32
5.3 Key Exchange Process between one hop distance nodes 32
5.4 Key Exchange Process between two hop distance nodes 33
5.5 RREQ message verification Request and Reply 34
5.6 RREP message verification Request and Reply 34

6.1 Analysis of key exchange between one hop neighbours 37
6.2 Analysis of key exchange between two hop neighbours 38
6.3 Peer Review process of RREQ packet 39
6.4 Peer Review process of RREP packet 40
6.5 Peer Review process in public key exchange between S and D 41

7.1 Comparison of Average Packet Transmission Delay vs Number of Packets 45

List of Tables

5.1 Table entries for one-hop nodes 33
5.2 Table entries for two-hop nodes 34

7.1 Comparison between NASRP and other existing secure routing protocols 44

List of Abbreviations

- MANET : Mobile Ad Hoc Network
- DSR: Dynamic Source Routing
- AODV: Ad Hoc on Demand Distance Vector
- CA: Certification Authority
- KDC: Key-Distribution Center
- RSA: Rivest, Shamir, and Adleman
- PDA: Personal Digital Assistant
- DoS: Denial of Service
- RREQ: Route Request
- RREP: Route Reply
- SAR: Security-Aware Routing
- SRP: Secure Routing Protocol
- SEAD: Secure Efficient Distance Vector
- PKI: Public-key Infrastructure

Chapter 1

Introduction

1.1 Introduction

"Ad Hoc" is a Latin phrase, which means "for this", meaning "for this special purpose only", by expansion it is a special network for a particular application. Mobile ad hoc network is infrastructure less network of mobile nodes (hosts) that are connected through the wireless links. In mobile ad hoc network, no central authority (node) is present which can control the network. Due to the resource constrain mobile ad hoc network faces lot of various challenges as compared to the wired network such as error prone broadcast channels, limited bandwidth, hidden and exposed terminal problems, frequent topology changes, power constraints and security issues [1].

Security issues is one of the greatest challenge in MANET. Mobile ad hoc network is more vulnerable due to its wireless channel and the lack of central authority. The security issues in MANET are mostly concentrated in two parts establishing secure route and securely data transmission. Routing protocol in MANET are not free from attacks. So to communicate securely we need to secure routing algorithm first unless only securing data communication can not provide security, safe and secure communication in mobile ad hoc network.

In this thesis work we consider secure routing algorithm and secure data transmission both the issues. So that before communication we can establish secure route for data delivery. In our proposed secure routing protocol, integrity, non-repudiation and confidentiality issues are taken into consideration which can prevent many security threat in mobile ad hoc communication.

Chapter Organization: section 1.2 describes the motivation, section 1.3 contains the objectives of the thesis, section 1.4 describes the thesis organization and section 1.5 contains summary of the chapter.

1.2 Motivation

After the study, we found that the presence of malicious node affects the communication process in MANET, which breaks integrity and confidentiality of the message. So the purpose of the communication is being violated. Due to the lack of central authority and wireless channel it is much more vulnerable. In any communication, routing protocol plays a great role to find the destination. This is the reason why attackers has chosen to attack routing protocol. If the attacker can modify the routing packets, it can modify the route. There are numbers of attacks are possible in MANET; those are Flooding Attack, Sleep Deprivation, Impersonation Attack, Black Hole Attack, Node Isolation Attack, Routing Table Poisoning Attack, Wormhole Attack, Location Disclosure Attack, Rushing Attacks, Blackmail, Snare Attack, The Invisible Node Attack. So to communicate securely in mobile ad hoc network we need to have a secure routing protocol.

1.3 Objective

Our objectives are:

- To design a secure routing protocol for mobile ad hoc network without the presence of central Authority (CA/KDC), which can maintain the

confidentiality, integrity and non-repudiation of the communication.

- To analysis the secure routing protocol against all possible attacks in mobile ad hoc network.
- Comparing our secure routing algorithm with other existing secure routing protocol.

1.4 Thesis Organization

The rest of the thesis is organized as follows: In Chapter 2, we discuss briefly about the Mobile Ad Hoc Network, various challenges in MANET and various possible security threats in MANET. In Chapter 3, we discuss about the literature surveys that have been done during the research work. In Chapter 4, we proposed a secure routing protocol called A Novel Approach of Secure Routing Algorithm; its design and architecture. In Chapter 5, we discuss about the analysis of our proposed secure routing protocol. In Chapter 6, we have given a comparison of our proposed secure routing protocol with existing secure routing protocols. Finally in chapter 7, we conclude our thesis.

1.5 Summary

In this chapter we have briefly describe the problem definition, motivation, objective of our thesis work and in the last section we have mentioned the organization of our thesis in subsequent chapters.

Chapter 2

Background Concepts

2.1 Introduction

Now a days mobility is becoming increasingly important for users of computing systems. Science and technology has made it possibly more powerful, smaller and less expensive wireless communicating devices (nodes). As a result users gain flexibility and the ability to exchange information and maintain connectivity while roaming through a wide area. The necessary support for mobile computing is being provided in some areas by installing base stations and access points. Mobile system users can maintain their connectivity by accessing this infrastructure from office, home or while on the road.

Mobile computing support is not available in all locations; due to high cost, low expected usage, or poor performance access points may not be set up . This may happen during outdoor conferences or in emergency situations like natural disasters and military services in inaccessible places. If mobile users wants to communicate without a support structure, they must form an ad hoc network. In this chapter, we look at mobile ad hoc networking in details. We present their applications, characteristics, analyse the complexities and design constraints associated with them and classify the existing routing algorithms in it.

Chapter Organization: Section 2.2 describes the brief about Mobile Ad Hoc Network, its applications, characteristics, complexity and design of MANET, section 2.3 describes the security issues in MANET, section 2.4 describes different types of attacks on ad hoc network routing protocols, section 2.5 describes routing protocol, sub section 2.5.1 describes AODV, subsection 2.5.2 describes DSR routing protocol and section 2.6 describes the summary of the chapter.

2.2 Mobile Ad Hoc Networks

A mobile ad hoc network (MANET), sometimes called a wireless ad hoc network or a wireless mesh network of mobile nodes, comprises of mobile computing devices (nodes) that uses wireless transmission for communication, without the presence of any established infrastructure or centralized authority or administration such as an access point in wireless local area network or a base station in cellular network [2]. The nodes are free to move randomly and organize arbitrarily; thus, the topology of the wireless network may change rapidly and unpredictably. Such type of network may operate in a standalone fashion, or it may be connected to the larger Internet. Unlike traditional mobile wireless networks, MANETs do not rely on any central coordinator but communicate in a self organized way. Mobile nodes can communicate to each other directly via wireless links if nodes are with in each other radio range, while nodes are far apart, should rely on other nodes to relay messages as routers. In mobile ad hoc network each node acts both as a host (capable of sending and receiving) and a router (forwards the data intended for some other node). Hence such networks sometime call as multi-hop wireless ad hoc networks. Figure 2.1 shows an example of mobile ad hoc network and its communication technology.

As shown in Figure 2.1, an ad hoc network might consist of several personal computing devices, including laptops, PDA, cellular phones, and so on. Each devices will be able to communicate directly with any other node in the network that resides

within its transmission range. For communicating with devices that reside beyond this range, the devise needs to use intermediate device to relay the messages hop by hop.

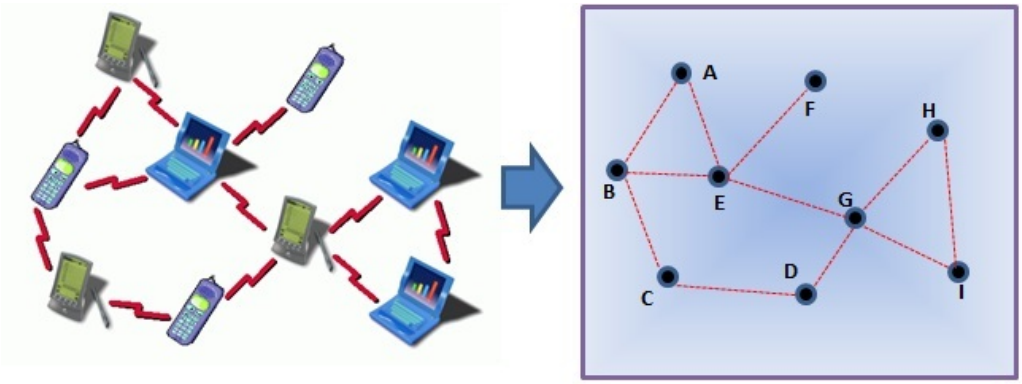

Figure 2.1: A Typical Mobile Ad Hoc Network

2.2.1 Application of Mobile Ad Hoc Network

Application of mobile ad hoc networks are numerous [3] [4]. Those are as follows

- Tactical networks
  - Military communication and operations
  - Automated battlefields
- Emergency services
  - Search and rescue operations
  - Disaster recovery
  - Replacement of fixed infrastructure in case of environmental disasters
  - Policing and fire fighting
  - Supporting doctors and nurses in hospitals
- Commercial and civilian environments

  - E-commerce: electronic payments any time and anywhere
  - Business: dynamic database access, mobile offices
  - Vehicular services: road or accident guidance, transmission of road and weather conditions, taxi cab network, inter-vehicle networks
  - Sports stadiums, trade fairs, shopping malls
  - Networks of visitors at airports

- Home and enterprise networking
  - Home/office wireless networking
  - Conferences, meeting rooms
  - Personal area networks (PAN), Personal networks (PN)
  - Networks at construction sites

- Education
  - Universities and campus settings
  - Virtual classrooms
  - Ad hoc communications during meetings or lectures

- Sensor networks
  - Home applications: smart sensors and actuators embedded in consumer electronics
  - Body area networks (BAN)
  - Data tracking of environmental conditions, animal movements, chemical/biological detection

- Coverage extension
  - Extending cellular network access
  - Linking up with the Internet, Intranets, etc.

2.2.2 Characteristics, Complexities and Design Constraints

Mobile ad hoc network eliminates the constraint of infrastructure set up and enable devices to create and join networks on the fly, any where, any time and virtually for any application. However, these flexibilities and convenience do come at a price. Mobile ad hoc networks inherit the common problems of wireless networking in general [5], and add their own constraints specific to ad hoc routing. Some of the notable characteristics, complexities and design constraints of MANETs are presented below [6]:

- **Dynamic and changing network topology:** In mobile ad hoc networks, because nodes can move arbitrarily, the network topology, which is typically multi-hop, can change frequently and unpredictably, resulting in route changes, frequent network partitions, and possibly packet losses.

- **Wireless medium:** In an ad hoc environment, nodes communicate wirelessly and share the same media (radio, infrared etc.). The wireless medium has neither absolute, nor readily observable boundaries outside of which the stations are unable to receive network frames. Thus the channel is unprotected from outside signals and hence it is significantly less reliable than wired media.

- **Limited availability of resources:** Because batteries carried by each mobile no have limited power supply, processing power is limited, which in turn lim services and applications that can be supported by each node. This becomes bigger issue in MANET because, since each node is acting as both an end syste and a router at the same time, additional energy is required to forward packets.

- **Autonomous and infrastructureless:** MANET does not depend on any established infrastructure or centralized administration. Each node operates in distributed peer-to-peer mode, acts as an independent router and generates independent data. Network management has to be distributed across different

nodes, which brings added difficulty in fault detection and management

2.3 Security Issues in Mobile Ad Hoc Networks

Mobile ad hoc network is not free from different active and passive attacks [7]. Due to the lack of central authority and resource constrains it is much more vulnerable. Depending upon the malicious node location attacks are classified into two different type, namely internal attacks and external attacks. And depending upon the operation it is also classified into two types, namely active attacks and passive attacks [8, 9].

2.3.1 Passive Attacks

A passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated. Detection of passive attack is very difficult since the operation of the network itself doesnt get affected. Details of different passive attacks in MANET are given below [7].

- **Eavesdropping:** It aims to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key, private key or even passwords of the nodes
- **Traffic Analysis and Monitoring:** Traffic analysis attack adversaries monitor packet transmission to infer important information such as a source, destination, and source-destination pair.

2.3.2 Active Attacks

An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks

can be internal or external. Details of different active attacks in MANET are given below [7].

- **Jamming attack:** Jamming is the particular class of DoS attacks. The objective of a jammer is to interfere with legitimate wireless communications. A jammer can achieve this goal by either preventing a real traffic source from sending out a packet, or by preventing the reception of legitimate packets.

- **Wormhole attack:** An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole.

- **Wormhole attack:** An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunnelled. This tunnel between two colluding attackers is referred as a wormhole.

- **Blackhole attack:** The black hole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding.

- **Byzantine:** A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.

- **Sybil attack:** If a malicious node impersonates some non-existent nodes, it will appear as several malicious nodes conspiring together, which is called a Sybil attack.

- **Fabrication:** Instead of modifying or interrupting the existing routing packets in the networks, malicious nodes also could fabricate their own packets to cause chaos in the network operations.
- **Modification:** In a message modification attack, adversaries make some changes to the routing messages, and thus endanger the integrity of the packets in the networks.
- **Repudiation:** Repudiation refers to a denial of participation in all or part of the communications.
- **Denial of service (DoS) attack:** Denial of service (DoS) is another type of attack, where the attacker injects a large amount of junk packets into the network. These packets overspend a significant portion of network resources, and introduce wireless channel contention and network contention in the MANET.
- **Gray hole attack:** The gray hole attack has two phases. In the first phase, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability.
- **Neighbor attack:** Upon receiving a packet, an intermediate node records its ID in the packet before forwarding the packet to the next node. However, if an attacker simply forwards the packet without recording its ID in the packet, it makes two nodes that are not within the communication range of each other believe that they are neighbour (i. e. one-hop away from each other), resulting in a disrupted route.
- **Jellyfish attack:** Similar to the black-hole attack, a jellyfish attacker first needs to intrude into the forwarding group and then it delay data packets unnecessarily for some amount of time before forwarding them.

2.4 Different type of attacks on ad hoc network routing protocols

Safe and secure communication is the great challenge in mobile ad hoc network. For secure communication, securing data is not only the solution; securing route discovery process is equally important. Because routing in MANET is not free from the attackers. Different types of possible attacks in routing protocol in MANET are as follows [8, 9].

- **Flooding Attack:**In flooding attack, malicious node continuously flood the route request packet, which results in denial of service.
- **Sleep Deprivation:** In this type of attacks malicious node/nodes keeps the other node/nodes busy by constantly engaging them in routing decision. Attacker node constantly request for route discovery for existing or non-existing destination nodes. As a result neighbouring nodes looses their battery power and bandwidth resources.
- **Black Hole Attack:**The black-hole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding.
- **Routing Table flooding Attack:**In this kind of attacks, malicious node continuously flood the route request packet for different node as a result routing table of the neighbour node becomes flooded
- **Wormhole Attack:**An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunnelled. This tunnel between two colluding attackers is referred as a wormhole.

- **Fabrication:** Instead of modifying or interrupting the existing routing packets in the networks, malicious nodes also could fabricate their own packets to cause chaos in the network operations.
- **Modification:** In a message modification attack, adversaries make some changes to the routing messages, and thus endanger the integrity of the packets in the networks.

2.5 Routing Protocol

Routing protocols in MANET specifies how nodes communicate with each other, routing information that enables them to select routes between any two nodes on a network. Routing algorithm determines the specific path of the route of communication, so the communication in the network depends on the efficiency and optimality of the routing algorithm. There are numerous routing available in the literature, in accordance of its route finding types it is two types; Proactive and Reactive [10].

Proactive Routing Protocol: All the routes to each destination are maintained in an up-to-date table. if any Changes made in the network topology are continually updated as they occur.

Reactive Routing Protocol: Route are only found when it is asked by the source node and route is maintained unless it is asked to terminate by the source node or after time exceed. In this section we will only discus AODV and DSR routing protocol. AODV and DSR both are proactive routing protocol [11, 12].

2.5.1 Ad Hoc on Demand Distance Vector (AODV) Routing Protocol

In AODV routing protocol, source node flood the route request (RREQ) to its neighbour nodes to reach the destination. Intermediate nodes check its destination

node if the node itself is not the destination then it rebroadcast the RREQ packet in similar manner until it reaches the destination. On receiving the RREQ, destination node generate the RREP packet and reply it through the reverse path in unicast manner [11].

RREQ packet contains the following specifications; Source Address, Destination Address, Source Sequence Number, Hop Count, Source Sequence Number, Destination Sequence Number, Broadcast Id (Request Id) and time-to-live (TTL) field.

Similarly RREP packet contains; Source Address, Destination Address, Sequence Number, TTL.

2.5.2 Dynamic Source Routing (DSR) Protocol

DSR routing protocol is almost similar to the AODV routing protocol, except that each intermediate node that broadcasts a route request(RREQ) packet adds its own address identifier to a list carried in the packet.

In DSR, RREQ packet contains; Address Sequence, Destination Address, Hop Count, Sequence Number and the RREP packet formate is similar to the RREQ except its propagated in unicast direction [12].

2.6 Summary

Mobile ad hoc network has lot of limitations; design constrains, resource limitation ,etc but still application of MANET network is numerous. Since there is no pre-existing infrastructure it suffers from many security threats. Now a days many security protocol is available in the literature to overcome this security threats. MANET network is vulnerable due to the lack of central authority or base station. MANET is a unstable network with constantly changing topology makes it more complex and challenging. But the use of mobile ad hoc network very vast, specially in the disaster management system, military services, ect.

Chapter 3

Literature Survey

3.1 Introduction

Providing security at the time of finding the route for communication in MANET is a challenging job. Many secure routing protocols are exist in the literature and research in this area is gaining increasing attention. In this chapter we briefly discuss the research conducted so far in secure routing protocol. There are number of secure routing protocol exists, but they are mostly based on certification authority (CA) or key distribution center (KDC) [14].

Chapter Organization: section 3.2 describes the literature survey of proposed work, section 3.3 describes the summary of the chapter.

3.2 Literature Survey

Our routing protocol is based on Dynamic Source Routing (DSR) and Ad Hoc on Demand Distance Vector Routing (AODV) [11, 12]. The route discovery process in DSR is almost similar to the AODV protocol, except that each intermediate node that broadcasts a route request (RREQ) packet adds its own address identifier to a list carried in the packet. The destination node generates a route reply (RREP) message that includes the list of addresses received in the route request and transmits

it back along this reverse path to the source. The details of most related paper of our research work are given bellow.

K.Sanzgiri and all; proposed secure routing protocol called ARAN, ARAN is a on-demand secure routing protocol [15]. It detects and protects against authentication, message integrity and non-repudiation. It uses asymmetric key cryptography. ARAN requires trusted certification server, The certificate accommodates the IP address of the node, its public key and a time-stamp of when the certificate was created and a time at which the certificate expires along with the signature by certification authority. But the disadvantages of ARAN is it uses the central authority (Certification Authority) and it can't protect against worm hole attack.

Adrian Perrig and all ; proposed secure routing protocol called ARIADNE, A secure on demand routing protocol for ad-hoc network (ARIADNE) is based on DSR routing protocol, it uses highly efficient symmetric cryptography [16]. It provides point-to-point authentication of a routing packets using a message authentication code (MAC) and a shared key between the two parties. For broadcasting RREQ packets it uses TESLA broadcast authentication protocol. TESLA keys are distributed to the participating nodes via an online key distribution center.

Yih-Chun Hu and all; proposed secure routing protocol called SEAD, Secure Efficient Ad-Hoc Distance Vector (SEAD) is based on destination-sequenced distance vector routing (DSDV) protocol [17].It is a proactive routing protocol. SEAD deals with attackers that modify routing information broadcast during the update phase of the routing information. SEAD makes use of efficient one-way hash chains rather than relying on expensive asymmetric cryptography operations. SEAD does not cope with wormhole attacks.

K.Sanzgiri and all; proposed routing protocol called A Secure Routing Protocol for Ad hoc Networks (SRP), relies on the availability of a security association (SA) between the source node and the destination node [18]. The SA could be established using a hybrid key distribution based on the public keys of the communicating

parties. Source and destination can exchange secret key using each others public key [19].

Manel Guerrero Zapata; proposed a routing protocol called Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing, it is a extension of AODV protocol [20]. The Secure AODV scheme is based on the assumption that each node possesses certified public keys of all network nodes. SAODV can be used to protect the route discovery mechanism of the AODV by providing security features like integrity, authentication and non repudiation. But in ad hoc network each node will know the others public key its a challenge.

Seung Yi and all; proposed a secure routing protocol called Security-Aware Ad-Hoc Routing (SAR) [21]. SAR is the generalized framework for any on demand ad-hoc routing protocol. SAR uses Key distribution or secret sharing mechanism. SAR may fail to find the route if the ad hoc network does not have a path on which all nodes on the path satisfy the security requirements in spite of being connected.

Panagiotis Papadimitratos and all; proposed secure routing protocol called Secure Link State Routing Protocol (SLSP) [22]. To function effectively without central key management authority, SLSP enables each node to periodically broadcast its public key to nodes within its zone. To achieve theses goals a Neighbor Lookup Protocol (NLP) is made an integral part of SLSP.

Ranga Ramanujan and all; proposed a secure routing protocol called Techniques for Intrusion-Resistant Ad Hoc Routing Algorithms (TIARA) [23]. TIARA mechanisms protect ad hoc networks against denial-of-service (DoS) attacks launched by malicious intruders. TIARA addresses two types of attacks on data traffic which are flow disruption and resource depletion. It requires online public key infrastructure.

Srdjan Capkun and all; proposed secure routing protocol called Building Secure Routing out of an Incomplete Set of Security Associations (BISS) [24]. The sender and The receiver can establish a secure route, even if, prior to the route discovery, only the receiver has security associations established with all the nodes on the

chosen route. It signs the request with its private key and includes its public key PKI in the request along with a certificate signed by the central authority binding its id with PKI.

Frank Kargl and all; proposed secure routing protocol called Secure Dynamic Source Routing (SDSR) Protocol [25]. It is based on DSR routing protocol. It checks the mutable and immutable field of the routing packets. and secure the authenticity of all nodes participating in a route .

A Sivakumar Kulasekaran and all; proposed a secure routing protocol called An efficient secure route discovery protocol for DSR [27]. It uses the peer review process to make to secure routing protocol secure but it uses only DSR routing protocol, packet size of the DSR routing protocol increase on passing by the intermediate nodes.

Phung Huu Phu and all; proposed a secure routing protocol called securing AODV routing protocol in MANET [28]. In this paper, each node tries to establish key exchange in with its neighbour but if any node provides any wrong information then it has to rely on it [29].

Calinescu Gruia; proposed a scheme to compute the two hop distance node in "Computing 2-Hop Neighborhoods in Ad Hoc Wireless Networks", it has been shown that a node can find out its two hop neighbour safe and securely. Bathini Eswar and all; uses two hop distance node to improve AODV Routing protocol [30].

3.3 Summary

Existing secure routing protocol are mostly based on some assumption but in all cases those assumptions can't be fulfilled. Many secure routing algorithms uses CA and KDC through online or offline. But if MANET network is established in such a area where no internet is available than these kinds of assumption fails. So we need to have a secure routing algorithm which can provide security in absence of internet or any other infrastructure.

Chapter 4

Proposed Scheme 1

4.1 Introduction

Routing protocol is the backbone in any communication network. In this chapter we have proposed a routing protocol called "Centralized Secure Routing Protocol for Mobile Ad Hoc Network" [31]. CSRP algorithm is based on Master Node (MN), which control the network, general node will be given a precomputed secret key, when nodes tries to become part of the network master node verifies the secret key. Based on the verification result if node passes the verification test it becomes the part of the network and in subsequent steps route establishment and data delivery is been done.

Chapter Organization: section 4.2 describes the details of CSRP algorithm, subsection 4.2.1 describes the description of CSRP algorithm, subsection 4.2.2 describes the design of CSRP, section 4.3 describes the architecture of CSRP, section 4.4 describes the summary of the chapter.

4.2 Proposed CSRP Algorithm

4.2.1 Description

In our proposed CSRP algorithm, the main idea is to create a safe and secure route for data communication from source to destination. In CSRP architecture, we have taken the concept of Master Node and the general nodes. The key idea of using MN in MANET architecture is to provide a robust secure routing protocol. MN is used as a trusted third party which is used for authenticating the nodes. If a node wants to communicate with another node in MANET then the MN will generate a session key between them. For generation of session key between two nodes N_1 and N_2, N_1 has to send request to MN for establishing a session key $K_{N_1N_2}$ with N_2 (neighbour). This process continues until we reach the destination. Then we flood the RREQ requests to the trusted neighbouring nodes. Then we continue the process until we reach the destination. We consider the RREQ which reach first and then we send a RREP from destination to source through the route taken by first RREQ. The data with the route as header is relayed by encrypting it with the session key of the two nodes and it is decrypted with the same session key on other end. This process continues till the destination is attained. This is how the data is relayed securely from source to destination.

4.2.2 Design

Node Recognition

The first step of CSRP algorithm is to recognize a node. This means, the nodes in an area set by the third party (organization) is to be recognized by MN to know whether the nodes are genuine nodes or malicious nodes. For this, organization places a pre-computed sign S and secret key S_K in the general nodes before placing the nodes in that area and it places a database of secret keys in MN. The public keys e, n and hash function are also placed in MN. S_K is common in MN and general

nodes. For recognition of genuine nodes by MN it verifies the SK first and then compute $h_1(S_K) = S^e$ mod n. If the $h(S_K)$ matches with $h_1(S_K)$ then it verifies it as a genuine node and then MN changes the S_K and places it again in the node. S_K changes with time interval. This modification helps in securing the key safe.

Algorithm 1 Node Recognition

1: Same S_K is shared by MN and each node individually
2: MN knows the public key of signing algorithm
3: MN compute $h(S_K)$
4: Sign S is pre-computed and placed in the general node along with S_K

$$\text{S} = [h(S_K)]^d \text{ mod n}$$

h = hash function known by both MN and general node
5: General node send request (S_K and S) to MN for verification
6: **if** S_K (send by general node) = S_K (stored in MN) **then**
7: $h_1(S_K) = S^e$ mod n
8: **if** $h(S_K) = h_1(S_K)$ **then**
9: Node is genuine
10: **else**
Malicious Node
11: **end if**
12: **else**
Malicious Node
13: **end if**
14: S_K changes with time interval

Connection Establishment and Secure Routing

The second step of our CSRP algorithm is to securely relay the data from source to destination. After recognizing the nodes by MN, the nodes establish session keys $K_{N_1N_2}$ between themselves. If source want to send data to destination it establishes

session keys between its neighbours and this process continues until we reach the destination. Then we check the Battery Power Status (BPS) of the nodes except source node and destination node. If BPS of a node is less than a threshold value (T) then RREQ request is not send to that node. By doing this we reduce the flooding of the packets, traffic in the network and power consumption. Then this process continues until we reach the destination and we choose the route covered by the first RREQ in the destination. Then a RREP is send from destination to sender and data delivery starts from source. Data delivery is done by encrypting the data with the session key and decrypting the data at other end. This encryption/decryption process continues and finally the data reaches the destination. If in case at the time of data delivery, an intermediate node fails then it searches for a new secure low cost route.

Algorithm 2 Centralized Secure Routing

1: After recognizing the nodes they will be the part of the network
2: Communication starts between source and the destination by establishing $K_{N_1N_2}$ between the nodes.
3: Check the BPS of the nodes
4: **if** $BPS \geq T$ **then**
    Send RREQ requests to those nodes (flooding)
5: **end if**
6: RREQ flooding continues until the destination comes
7: Choose the first RREQ and send RREP through that route from destination to source
8: Data is relayed by encrypting the data by $K_{N_1N_2}$ and decryption is done by the same $K_{N_1N_2}$ at other end
9: Encryption/Decryption process continues until destination comes

4.3 CSRP Architecture

CSRP gives a robust secure routing in the network. Here we have presented the working of CSRP and its performance with the help of an architecture. Figure 4.1 shows the CSRP architecture and the common secret keys which changes with respect to time. Table 4.1 shows the table of secret keys. Figure 4.2 shows how two nodes establish a session key. This process continues and every node establishes a session key with its neighbouring nodes. Figure 4.3 presents that the key are established. After session key establishment the source node broadcasts RREQ and this process continues until RREQ reaches the destination. Then a RREP is send from destination to source from that route in which RREQ comes first. Then the data is delivered from the source in that route by encrypting it with the session key of two neighbouring nodes in that route. Then this data is decrypted using the same session key and this process continues until the data reaches destination. Figure 4.4 shows the flooding of RREQ and RREP from D to S. Figure 4.5 shows the data delivery by encryption and decryption using session key. We know that MANET is hugely affected by Spoofing attack, Black-hole attack, Wormhole attack, Byzantine attack , [5] etc. which degrades the network performance. So, this architecture helps in securing the data against these active and passive attacks and provides a secure routing environment.

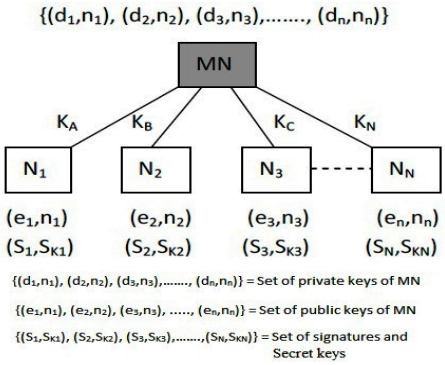

Figure 4.1: CSRP architecture with secret keys

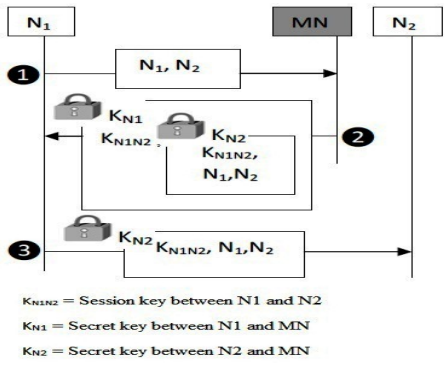

Figure 4.2: Session Key establishment

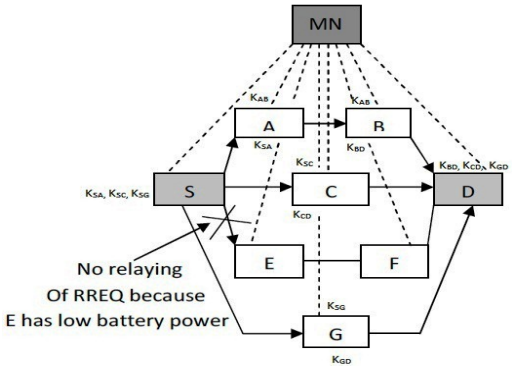

Figure 4.3: Session Key established between the nodes

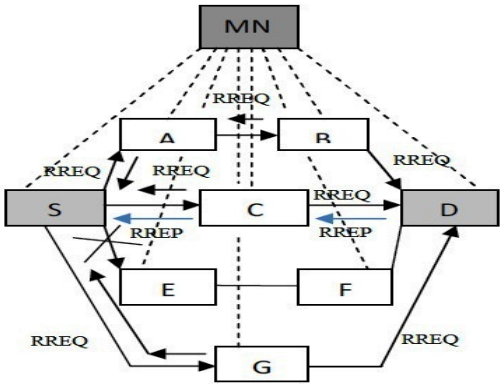

Figure 4.4: Flooding of RREQ to D and RREP from D to S

Table 4.1: Secret Key Table

Used Secret Key	Changed Secret Key
S_{K_1}	K_A
S_{K_2}	K_B
S_{K_3}	K_C
S_{K_1}	K_A
.	.
S_{K_N}	K_N

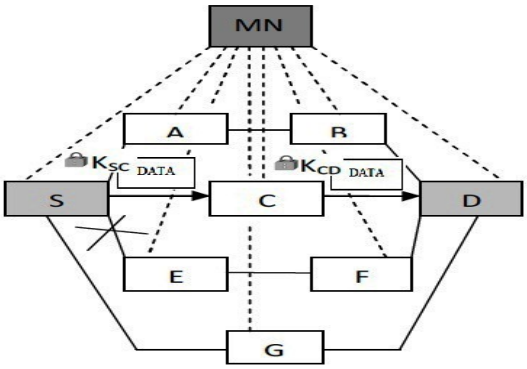

Figure 4.5: Data delivery by encryption and decryption using session key

4.4 Summary

CSRP algorithm is mainly for very secure communication like, military or any secure services, where the nodes are given secret before deploying it to the remote places. Any communication, where security needs is very high but infrastructure is present or not enough there CSRP routing algorithm would be good option.

Chapter 5

Proposed Scheme 2

5.1 Introduction

Security in routing protocol in MANET is very essential. No existing secure routing protocol is fully capable of preventing all security threats. In this chapter, we propose secure routing algorithm called A Novel Approach of Secure Routing Protocol (NASRP) to guarantee the integrity, non-repudiation and confidentiality of routing packets without the presence of central authority. In our approach, it has three steps; in the first step, each node perform a key exchange operation with its one and two hop distance neighbours, in the second step, secure route establishment and in the third step, secure data communication is performed. Key exchange operation is done in two steps; in the first step, source node (S) exchanges public key (e) with its one hop distance nodes and establish a secret key (S_K), and in the second step, source node exchanges public key with its two hop distance nodes and establish a secret key. On establishing the key exchange process node can participate in routing process. In route establishment process, secure route will be established between the sender and receiver. In the third step, sender and receiver will exchange their public key securely and establish a secret key for communication and then data communication is performed.

Chapter Organization: section 5.2 describes our proposed secure routing protocol called "A Novel Approach of Secure Routing protocol", subsection 5.2.2 describes details of NASRP, subsection 5.2.3 describes design of NASRP protocol, subsection 5.2.4 describes the architecture of NASRP protocol, section 5.3 describes summary of the chapter.

5.2 A Novel Approach of Secure Routing Protocol

5.2.1 Preliminaries

In our proposed protocol, A Novel Approach of Secure Routing Protocol (NASRP), primary idea is to create a safe and secure path (route) for data communication between nodes. NASRP is a intermediate of AODV and SRP protocol. It follows all the steps of AODV. Unlike DSR, NASRP contains only two address fields in the routing packets where DSR accommodates all the intermediate nodes in the routing packets. Figure 5.1 shows the format of the NASRP routing protocol where "DA" represents Destination Address, "SA" represents Source Address, "HC" represents Hop Count and "SN" represents Sequence Number. In NASRP, two address fields is required, one is for accommodating super sender of packet with respect to the present node and other is for sender of the packet. We have considered all nodes follows RSA as public key crypto-system and every node has its own public key (e) and private key (d), symmetric key algorithm and hash algorithm. NASRP provides integrity, non-repudiation to the routing packets.

5.2.2 Description

In NASRP architecture, the key idea is to provide security to the routing protocol without the presence of central authority (CA/KDC). Each node in the network negotiates public key with its one hope distance neighbours and two hope distance

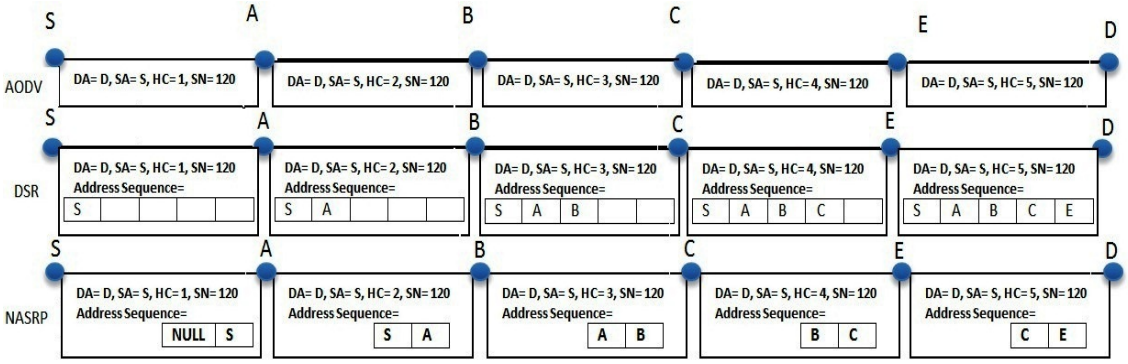

Figure 5.1: RREQ Packet format of AODV, DSR and NASRP

neighbours [30] [32]. With the help of public key each node establish a secret key to its one hope and two hopes distance neighbours by RSA public key crypto-system. After completing the negotiation and key agreements nodes are eligible to participate in communication. For data communication sender node initiates the route finding process to reach the destination node by generating and broadcasting route request (RREQ) packet. During the propagation of RREQ packet, each packet is verified by its previous two hope distance sender node and if it is maintained the integrity then the packet to be forwarded to next suitable node in the path.

Once RREQ packet reaches the destination and successfully verified, destination node generates route reply packet (RREP) and propagate it in the same route by following the similar verification process.

5.2.3 Design

The primary goal of NASRP scheme is to guarantee the integrity and non-repudiation of routing messages so that the protocol can prevent many different kinds of active and passive attacks. Our protocol has three different steps to provide security, in the first stage key agreement process between one hop and two hope distance neighbours, in the second stage route request and route reply, and in the last stage public key exchange between the source and destination node and data

communication. Details of the each steps are given bellow.

Key agreement between one hop distance neighbours

In the key agreement between one hop neighbours process, each node sends its public key (e_s) and a sing of hash of public key ($hash(e_s)^{d_s}$) to its one hop distance neighbours. Neighbour node receive the request and verify it. After verifying the packet, it generates a reply message which contains the public key (e_n) and a sing MDC (Modification Detection Code) of public key ($hash(e_n)^{d_n}$) of itself. After completing the negotiation of public key, initiator node generates a secret key (S_K) and send it by encrypting the receiver's public key ($encrypt_{e_n}(S_K)$). The steps are shown bellow, where S represents source node and N_1 represents one hop distance node and "$\rightarrow$" represents direction of communication.

1. $S \rightarrow N_1 : <Key\_Agreement\_Req, Request\_Id, Sender\_Addr, e_S, hash(e_S)^{d_S}>$
2. $N_1 \rightarrow S : <Key\_Agreement\_Rep, Request\_Id, Sender\_Addr, Neighbour\_Addr, e_{N_1}, hash(e_{N_1})^{d_{N_1}}>^{e_S}$
3. Sender Node (S) generate a secret key (S_K)
4. $S \rightarrow N_1 : < Key\_Offer\_Req, Request\_Id, (S_K), hash(S_K) >^{e_{N_1}}$
5. $N_1 \rightarrow S : < Key\_Offer\_Rep, Request\_Id, hash_{S_K}(Request\_Id) >^{e_s}$

Key agreement between two hop distance neighbours

In the key agreement process of two hop distance nodes, each node gather information about the two hope neighbours and sends its public key (e_S) and a sing of MDC of public key ($hash(e_S)^{d_S}$) to its two hop distance neighbours. After receiving the request neighbour node verify it and send acknowledgement, which contains Request Id, Sender and Neighbour address, Public Key(e_{N_2}) of itself, a sing of MDC of public key ($hash(e_{N_2})^{d_{N_2}}$) of the neighbour and the sing of MDC of public key ($hash(e_S)^{d_S}$) of the sender. The detail process are shown bellow,

where S represents source node, N_2 represents two hop distance neighbour and "$\rightarrow$" represents direction of communication.

1. $S \rightarrow N_2 : <Key\_Agreement\_Req, Request\_Id, Sender\_Addr, (e_S), hash(e_S)^{d_S}>$
2. $N_2 \rightarrow S : <Key\_Agreement\_Rep, Request\_Id, Sender\_Addr, Neighbour\_Addr, (e_{N_2}),\ hash(e_{N_2})^{d_{N_2}},\ hash(e_S)^{d_S}>^{e_S}$
3. Source Node (S) Generate a secret key S_K
4. $S \rightarrow N_2 : < Key\_Offer\_Req, Request\_Id, (S_K), hash(S_K) >^{e_{N_2}}$
5. $N_2 \rightarrow S : < Key\_Offer\_Rep, Request\_Id, hash_{S_K}(Request\_Id) >^{e_S}$

Route Request

For finding the route, source node, say S generate the route request(RREQ) packet and broadcasts it. RREQ message is propagated by the intermediates nodes until it reaches the destination node (D). After receiving RREQ message, intermediate node (I) checks whether the message needs to be re-broadcast or not. If it is needed to be re-broadcast it sends a message authentication request (unicast) to the super sender of the RREQ message. On receiving the message authentication request, super sender create a MAC (Message Authentication Code) of RREQ message ($hash_{S_K}(RREQ)$) by using the secret key (S_K) and encrypting it using the intermediates public key (e_I) and then send the entire message ($hash_{S_K}(RREQ)^{e_I}$) to the intermediate node. This process continues until the RREQ reaches the destination node. Lets A, B and C are three consecutive nodes, where A is source and B and C are the intermediate node through which packets are relaid. On receiving the route request, B doesn't check it's integrity because its directly coming from the source node but C will check it by doing following steps.

1. $C \rightarrow A : <RREQ\_Authen\_Req,\ Broadcast\_Id, Sequence\_Number, Sender\_Addr>^{e_A}$

2. $A \rightarrow C$: $<RREQ\_Authen\_Rep,\ Broadcast\_Id,\ Sender\_Addr,\ Super\_Sender\_Addr,\ hash_{S_K}(RREQ)>^{e_C}$

Route Reply

On receiving the route request, destination node (D), generates route reply (RREP) message and send it (unicast) through the reverse path of the arrival path. During the propagation of the RREP packet, intermediate nodes check the authenticity and integrity of the route reply message in the similar way of authentication of RREQ message. Let X, Y and D are three nodes where D is destination node, which sending route reply packet through Y and X path. X is te one hop distance node so the there is no need of checking the integrity of the packet. Y is two hop distance node so it will check the integrity of the message by sending the authentication request. steps are shown bellow,

1. $Y \rightarrow D$: $<RREP\_Authen\_Req,\ Broadcast\_Id,\ Sequence\_Number,\ Sender\_Addr>^{e_D}$

2. $D \rightarrow Y$: $<RREP\_Authen\_Rep,\ broadcast\_Id,\ Sender\_Addr,\ Super\_Sender\_Addr,\ hash_{S_K}(RREP)>^{e_Y}$

Route Maintenance

In route maintenance process, during route finding if destination node is un reachable then a error message (RERR) is generated and propagated to the source node. During the RERR message propagation, it follows the message authentication process. Authentication steps are shown bellow. Let P,Q and R three nodes and R is the error message (RERR) generator, and it will propagate through p and Q nodes, steps are as follows,

1. $Q \rightarrow R$: $<RERR\_Authen\_Req,\ Host\_Unreachable\_Id,\ Sender\_Addr>^{e_R}$

2. $R \rightarrow Q$: $<RERR\_Authen\_Rep,\ Host\_Unreachable\_Id,\ Sender\_Addr,\ Super\_Sender\_Addr,\ hash_{S_K}(REER)>^{e_Q}$

Data Communication Between Source and Destination

- **Public Key Exchange:** Before start data communication source (S) and destination node (D) must know the public key of each other. To exchange the public key we considered the similar to RREQ message authentication process during the propagation of key exchange message

  1. $S \rightarrow D$: $<Destin\_Addr,(e_S),\ hash(e_S)>$
  2. $D \rightarrow S$: $<Destin\_Addr,(e_D),\ hash(e_D)>^{e_S}$

- **Data Packet Exchange:** On receiving the public key, source node (S) generate a share key (sh_K) and encrypt ($(sh_K)^{e_d}$) it by destinations public key (e_d) and sends it followed by the data packet. On receiving the key packet, destination node decrypt it and get the shared key. Destination node decrypt all rest of the packets by using the shared key. The detail steps are shown bellow.

  1. $S \rightarrow D$:
     - for secret key: $< S_K >^{e_D}$
     - for data packet: $< data >^{S_K}$

5.2.4 Architecture

To describe the architecture of our proposed we have considered a MANET network, shown in Figure 5.2, the network consist of {A, B, C, ..., K} nodes. We discuss the details of each steps of our proposed routing protocol.

In the first step of key exachange operation: each node perform key exchange operation with its one hop distance neighbour nodes; first each node exchange public key and then a shared secret key. The key negotiation process are shown in Figure 5.3

After negotiation and key exchange each node make a entry table, each node maintain a table to keep record of the details of its one hop distance nodes. It keeps

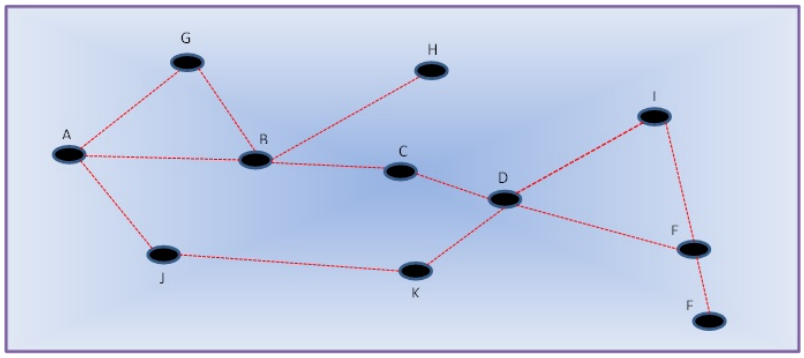

Figure 5.2: A MANET network

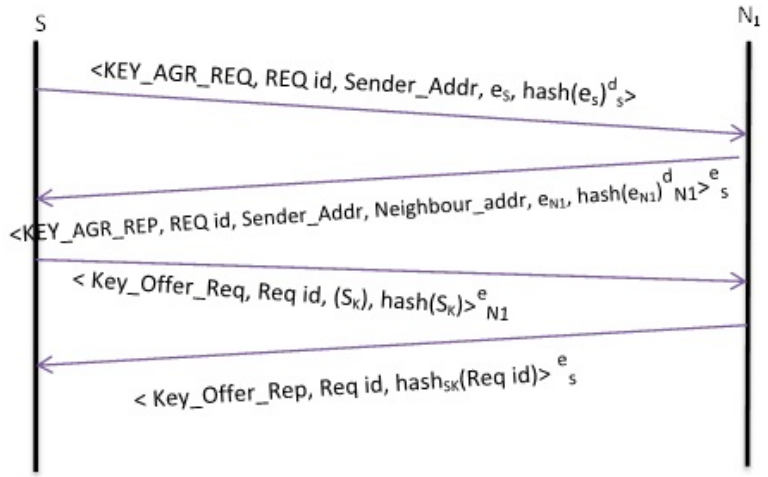

Figure 5.3: Key Exchange Process between one hop distance nodes

the record of Node Id, Public key and Secret key. From the above network (Figure 5.2), we took an example of node "B" and shown the table entry for all of its one hop neighbours, Table 5.2 shows the entry for its one hop distance neighbours.

In the second step of key exchange operation: each node exchange their public key and a share key with its two hope distance neighbours. The details of negotiation and key exchange operation are shown in Figure 5.4, where N_1 and N_2 represents one and two hop distance neighbour respectively.

For each negotiation and key exchange, node will make a entry in the Table. Each node maintain a table to keep record of the details of its two hop distance

Table 5.1: Table entries for one-hop nodes

Node ID	Public Key (e)	Secret Key (S_K)
A	e_A	S_{K_1}
C	e_B	S_{K_2}
G	e_C	S_{K_3}
H	e_D	S_{K_4}

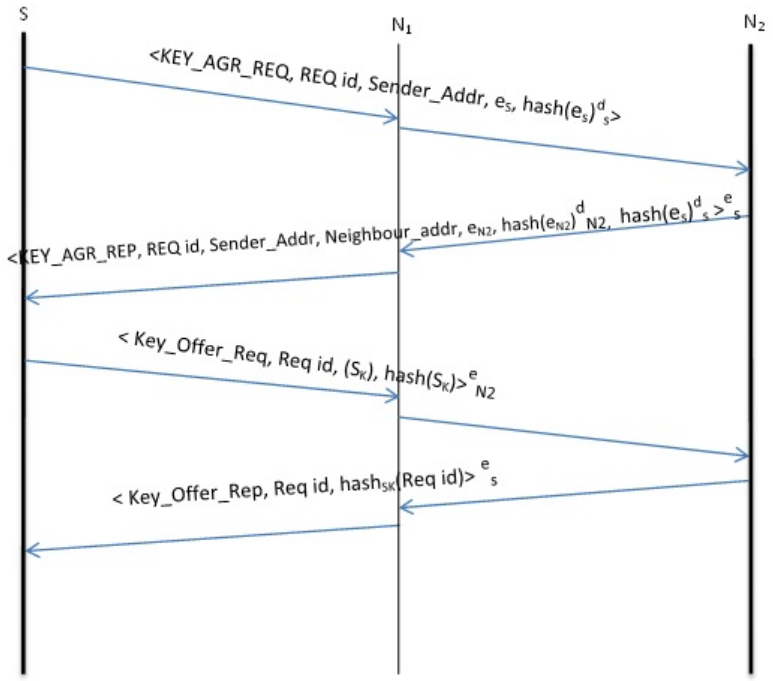

Figure 5.4: Key Exchange Process between two hop distance nodes

neighbour nodes. From the above network (Figure 5.2), we took an example of node "C" and makes the table entry for all of it's two hop neighbours, Table 5.2 shows the entry for it's two hop distance neighbours.

RREQ and RREP packet forwarding: In the network (Figure 5.2), if node A, wants to send the data to node F, then route request (RREQ) packet is to be generated and broadcast to find the route to reach the destination. During the

Table 5.2: Table entries for two-hop nodes

Node ID	Intermediate Node	Public Key (e)	Secret Key (SK)
A	B	e_A	S_{K_1}
G	B	e_G	S_{K_2}
H	B	e_H	S_{K_3}
E	D	e_E	S_{K_4}
I	D	e_I	S_{K_5}
K	D	e_K	S_{K_6}

propagation of RREQ packet each time it will be reviewed by it two hop distance away sender. If is satisfy the review process then only it will be propagated to the farther nodes. The process are shown in Figure 5.5. Similarly, during route reply and route maintenance each RREP and RERR packet will be verified by peer review process by it two hop distance sender. Figure 5.6 shows the detail of route reply process.

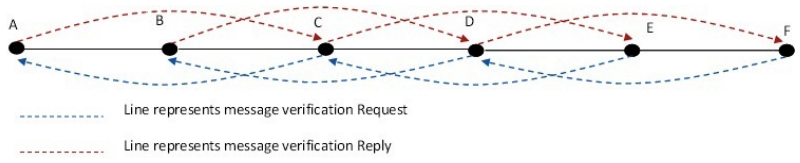

Figure 5.5: RREQ message verification Request and Reply

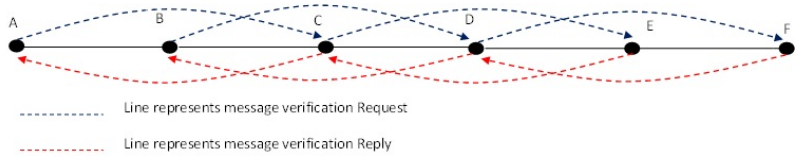

Figure 5.6: RREP message verification Request and Reply

5.3 Summary

In this chapter each steps of design and architecture of our proposed NASRP protocol are carefully shown. It preserves integrity, non-repudiation and confidentiality of Routing packets as well as data packets. Our proposed algorithm follows a peer review process and important point of our proposed algorithm is it doesn't use any central authority neither in online nor in offline.

Chapter 6

Proposed Model Analysis

6.1 Introduction

NASRP scheme mainly guarantee integrity and non repudiation which leads to prevention of many security threats of MANET routing protocol. In this section we will analyse each steps of our proposed secure routing protocol (NASRP). First we will discus the security measure of key exchange between one hop and two hop distance nodes. In the second step we will discus the security measure of routing information exchange and in the last step we will discus the security measure of data packet transmission.

Chapter Organization: section 6.2 describes the analysis of NASRP protocol, subsection 6.2.1 describes correctness key exchange between neighbours, subsection 6.2.2 describes the correctness of RREQ packets, subsection 6.2.3 describes the correctness of RREP packets, subsection 6.2.4 describes correctness of data packet transmission and section 6.3 describes summary of the chapters.

6.2 Analysis

6.2.1 Key Exchange between Neighbours

Analysis of Public and Secret Key exchange between one hop neighbours

In the analysis of the key exchange process between one hop neighbours , we will make a proof of key exchange operation. Figure 6.1 shows the proof of key exchange operation between the one hop distance neighbours, where public key and secret key are securely negotiated.

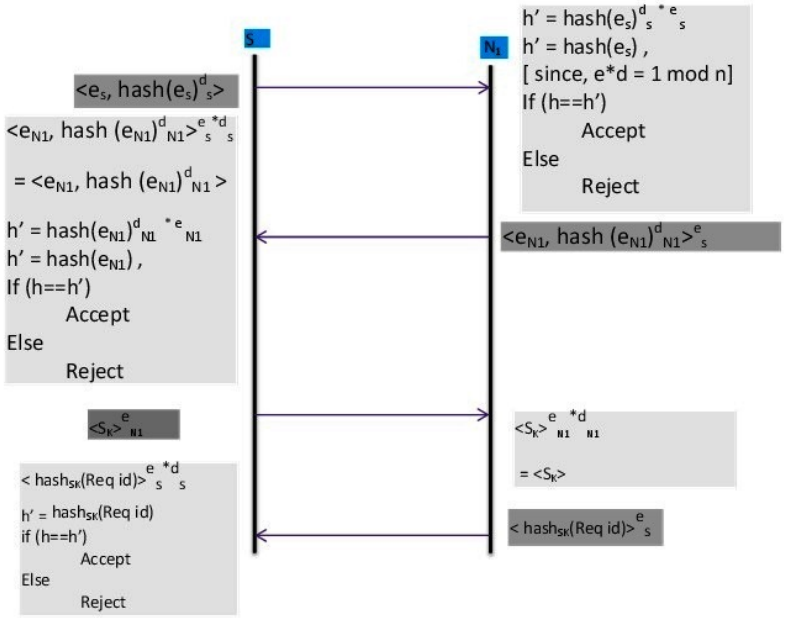

Figure 6.1: Analysis of key exchange between one hop neighbours

Analysis of Public and Secret Key exchange between two hop neighbours

The analysis of Key exchange between two hop neighbours shown in Figure 6.2, where public key and secret keys are securely transferred. If intermediate node (N_1) node modifies the packet, then two situation can arise, first, if the node changes the public key only and second, if it change the public key and sing of hash of public key.

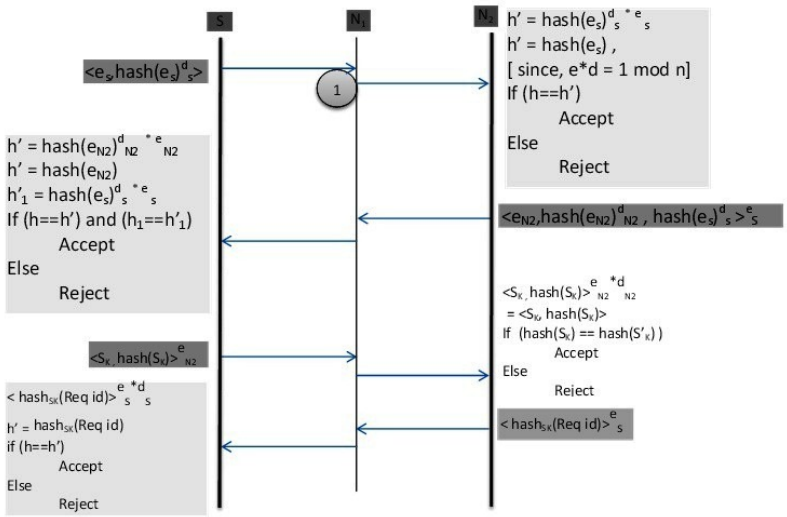

Figure 6.2: Analysis of key exchange between two hop neighbours

1. **Condition 1: if N_1 node alters the public key only:** If N_1, alters the public, say e_1 is the modified public key, we can prove that it will not pass the verification process in the destination node.

   - $S \rightarrow D : < e_S, hash(e_S)^{d_S} >$
   - After modification public key becomes e_S^1
   - $h^1 = hash(e_S)^{d_S * e_S^1}$
   - $h = hash(e_S^1)$, hence, $h_1 \neq h$

2. **Condition 2: if N_1 node alters the public key and sing of hash of it:** If the node N_1 alters public key and sign both, we can prove that it will not pass the verification process in the destination node.

   - $S \rightarrow D : < e_S, hash(e_S)^{d_S} >$
   - After modification public key becomes e_S^1 and $hash(e_S^1)^{d_S^1} = h^1$
   - since, it will be transmitted to the source node
   - source node will compare, $hash(e_S^1)^{d_S^1}$ and $e_S, hash(e_S)^{d_S}$
   - hence, $h_1 \neq h$

6.2.2 Analysis of RREQ packets

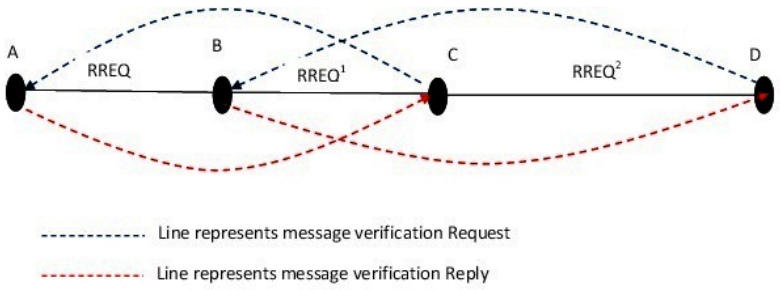

Figure 6.3: Peer Review process of RREQ packet

Lets A,B,C are three nodes, A send route request packet say RREQ to B. On receiving RREQ packet, B send it to C, say now the packet is $RREQ^1$. Now, node C will verify the packet integrity by the following process.

1. $A \rightarrow B : RREQ$
2. $B \rightarrow C : RREQ^1$
3. $C \rightarrow A : < Verify\_RREQ, Sequence\_No >^{e_A}$
4. $A \rightarrow C : < RREQ, hash_{S_K}(RREQ) >^{e_C}$
5. $< RREQ, hash_{S_K}(RREQ) >^{e_C * d_C} = < RREQ, hash_{S_K}(RREQ) >$
6. $h = hash_{S_K}(RREQ)$
7. $if(h == hash_{S_K}(RREQ))$ then *Accept*
8. *else Reject*
9. end if
10. After verifying the MDC, Node C will do the following
11. if($RREQ^1 \rightarrow Destin\_addr = RREQ \rightarrow Destin\_addr$)

12. if $((RREQ^1 \rightarrow hop\_count - RREQ \rightarrow hop\_count) = +1)$

13. if $((RREQ^1 \rightarrow Addr\_Seq - (RREQ^1 \rightarrow Addr\_Seq \cap RREQ \rightarrow Addr\_Seq)) == RREQ \rightarrow Sender\_Addr)$

14. Route Request is Genuine

6.2.3 Analysis of RREP packets

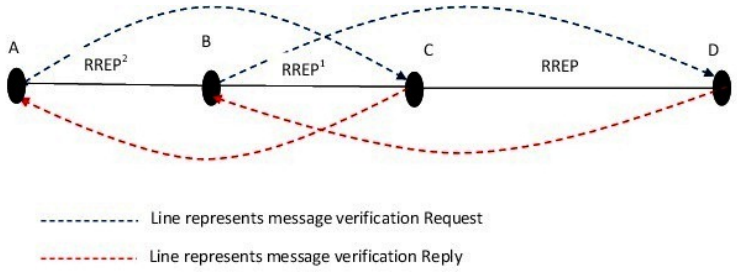

Figure 6.4: Peer Review process of RREP packet

On receiving the RREQ packet, destination node sends the route reply packet (RREP) in similar fashion. Process are shown bellow.

1. $D \rightarrow C : RREP$
2. $C \rightarrow B : RREP^1$
3. $B \rightarrow D : < Verify\_RREP, Sequence\_No >^{e_D}$
4. $D \rightarrow B : < RREP, hash_{S_K}(RREP) >^{e_B}$
5. $< RREP, hash_{S_K}(RREP) >^{e_B * d_B} = < RREP, hash_{S_K}(RREP) >$
6. $h = hash_{S_K}(RREP)$
7. $if(h == hash_{S_K}(RREP))$ then *Accept*
8. *else Reject*

9. end if
10. After verifying the MDC, Node B will do the following
11. if($RREP^1 \rightarrow Destin\_addr = RREP \rightarrow Destin\_addr$)
12. if $((RREP^1 \rightarrow hop\_count - RREP \rightarrow hop\_count) == +1)$
13. if $((RREP^1 \rightarrow Addr\_Seq - (RREP^1 \rightarrow Addr\_Seq \cap RREP \rightarrow Addr\_Seq)) == RREP \rightarrow Sender\_Addr)$
14. Route Reply is Genuine

6.2.4 Analysis of Data packet Transmission

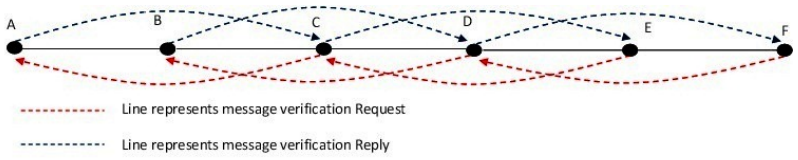

Figure 6.5: Peer Review process in public key exchange between S and D

Data packet transmission start in two steps; in the first steps source node and destination node exchange the public key by using peer review process and in the second step a secret key will be sent to the destination by encrypting it by destination's public key followed by data packet encrypted by secret key

- Public key exchange:
- $A \rightarrow B : e_s, hash(e_s)$
- $B \rightarrow C : e_s, hash(e_s)$
- $C \rightarrow A : < Verify\_Packet >^{e_a}$
- $A \rightarrow C : < hash(e_s) >^{e_c}$

  - $< hashe_s >^{e_c * d_c} = < hash(e_s) >= h'$
  - $if(h == hash(e_s))$
  - $Accept$
  - $else$
  - $Reject$
  - end if

- $S \rightarrow D : (S_K)^e_d$
  - $(S_K)^{e_d * d_d} = S_K$
- $S \rightarrow D : (data)^{S_K}$
  - $(data)^{S_K} = data^1$
  - $(data^1)^{S_K}$=data

6.3 Summary

In this Chapter, we have mathematically proved the integrity, non-repudiation and confidentiality is being maintained during the packet transmission. In each step of analysis, correctness of the each step of NASRP protocol are carefully described.

Chapter 7

Comparison

7.1 Introduction

In this section, we have compared our proposed routing algorithm with the popular existing routing algorithm. we have taken some security threats and analyse those security threats in our proposed routing protocol with the existing secure routing protocols.

Chapter Organization: section 6.2 describes the comparison of our routing protocol with the existing routing protocols, section 7.3 describes the average end-to-end delay comparison between AODV and NASRP, section 7.4 decries the summary of the chapter.

7.2 Comparison with other secure routing protocols

We have compared our proposed (NASRP) protocol with the existing popular routing protocols. The comparison is based on security threats, encryption algorithm, MANET Protocol are shown in Table 7.1. In comparison we have shown our proposed protocol is providing integrity, non-repudiation and confidentiality but

the central advantage of our protocol is it doesn't need any central authority.

Table 7.1: Comparison between NASRP and other existing secure routing protocols

Protocol	SAOVD	ARAN	ARIADNE	SEAD	**NASRP (Proposed)**
Type	Reactive	Reactive	Reactive	Proactive	**Reactive**
Encryption Algorithm	Asymmetric	Asymmetric	Symmetric	Symmetric	**Asymmetric /Symmetric**
MANET Protocol	AODV	AODV/DSR	DSR	DSDV	**DSR/AODV (Modified)**
Central Trust Authority	Certificate Authority (CA)	Certificate Authority (CA)	Key Distribution Center (KDC)	Certificate Authority (CA)	**No Central Authority**
Authentication	Yes	Yes	Yes	Yes	**Yes**
Confidentiality	No	Yes	No	No	**Yes**
Integrity	Yes	Yes	Yes	No	**Yes**
Non Repudiation	Yes	Yes	No	No	**Yes**
Anti-Spoofing	Yes	Yes	Yes	No	**No**
Dos Attacks	No	No	Yes	Yes	**No**
Black-hole Attacks	No	No	No	No	**No**

7.3 Average Transmission Delay Comparison

In this section we have compared our secure routing protocol with AODV routing protocol with respect to the average end-to end transmission delay. We have

considered 15 node in the area of 500m X 500m. We have considered the channel bandwidth is 11 Mbps and packet size 512 KB. We have simulated the our algorithm with 50, 100,150,200 and 250 number of packets and took average of it. Figure 7.1 shows the bar graph of average packet transmission delay vs number of packets.

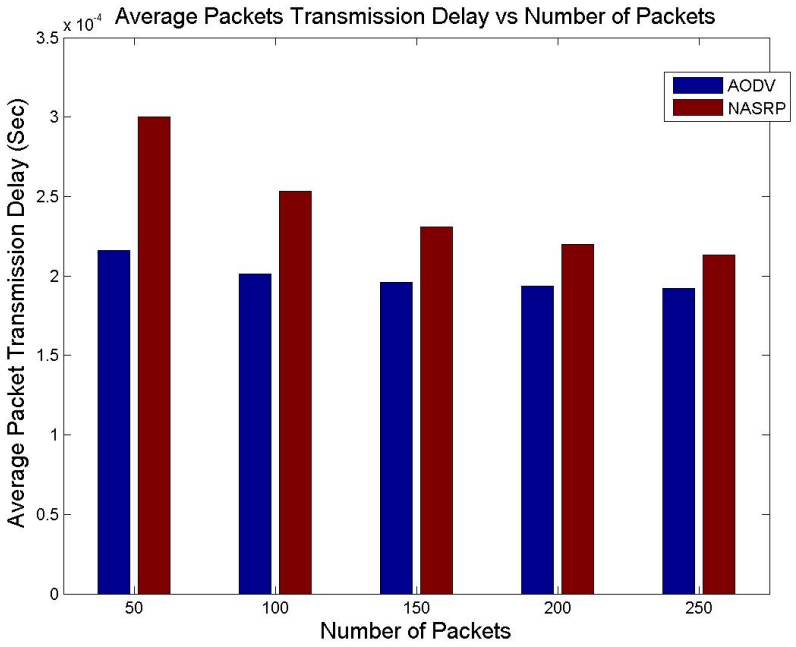

Figure 7.1: Comparison of Average Packet Transmission Delay vs Number of Packets

7.4 Summary

Our proposed routing protocol, prevents many security threats like, Authentication, Confidentiality, Integrity, Non Repudiation, etc. But there are some threats which can not be prevented in NASRP secure routing protocol. But the central issue is it does not use Certification Authority (CA) or Key-Distribution Center (KDC).

Chapter 8

Conclusion and Future Works

8.1 Conclusion

The lack of central authority and dynamic topology makes MANET network more vulnerable. Our proposed secure routing protocol, CSRP provides security in closed environment where high security is needed and all nodes deployed in the area are from single authority and NASRP provides mainly integrity, non-repudiation and confidentiality to the communication of the MANET networks. But NASRP, can't prevent back-hole , Byzantine like attacks which drops the packet with some certain probability or entirely. Our protocol has a limitation, if there is two malicious node in the routing path in the network, the secure protocol may violates. It mainly works in a types of network where no two malicious node presents consecutively.

8.2 Future Work

Secure routing protocol with prevention of all attacks still a open challenge problem. But in our proposed routing protocol we can add trust evaluation feature which can prevent packet-dropping attacks like black-hole, Byzantine, etc. each node will calculate the trust of its neighbour nodes and based on the trust value, it will be decided that the node will be part of the network of not.

Bibliography

[1] Mourad Elhadef, Azzedine Boukerche, and Hisham Elkadiki. Diagnosing mobile ad-hoc networks: two distributed comparison-based self-diagnosis protocols. In *Proceedings of the 4th ACM international workshop on Mobility management and wireless access*, pages 18–27. ACM, 2006.

[2] George Aggelou. *Mobile Ad Hoc Networks.* Tata McGraw-Hill, 2009.

[3] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, and Piet Demeester. An overview of mobile ad hoc networks: Applications and challenges. *JOURNAL-COMMUNICATIONS NETWORK*, 3(3):60–66, 2004.

[4] Humayun Bakht. Applications of mobile ad-hoc networks. *http://www.computingunplugged.com/issues/issue2004 09/00001371001.html*, 2004.

[5] Samba Sesay, Zongkai Yang, and Jianhua He. A survey on mobile ad hoc wireless network. *Information Technology Journal*, 3(2):168–175, 2004.

[6] Imrich Chlamtac, Marco Conti, and Jennifer J-N Liu. Mobile ad hoc networking: imperatives and challenges. *Ad Hoc Networks*, 1(1):13–64, 2003.

[7] Sudhir Agrawal, Sanjeev Jain, and Sanjeev Sharma. A survey of routing attacks and security measures in mobile ad-hoc networks. *arXiv preprint arXiv:1105.5623*, 2011.

[8] POWAH YAU, Shenglan Hu, and Chris J Mitchell. Malicious attacks on ad hoc network routing protocols. *Information Security Group.*

[9] Djamel Djenouri, L Khelladi, and N Badache. A survey of security issues in mobile ad hoc networks. *IEEE communications surveys*, 7(4), 2005.

[10] Petteri Kuosmanen. Classification of ad hoc routing protocols. *Finnish Defence Forces, Naval Academy, Finland, petteri. kuosmanen@ mil. fi*, 2002.

[11] C.E. Perkins and E.M. Royer. Ad-hoc on-demand distance vector routing. In *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on*, pages 90–100, 1999.

[12] David B Johnson, David A Maltz, Josh Broch, et al. Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks. *Ad hoc networking*, 5:139–172, 2001.

[13] I. Woungang, S.K. Dhurandher, M.S. Obaidat, Han-Chieh Chao, and C. Liu. Trust-enhanced message security protocol for mobile ad hoc networks. In *Communications (ICC), 2012 IEEE International Conference on*, pages 988–992, 2012.

[14] Ranvijay Karan Singh, Rama Shankar Yadav. A review paper on ad hoc network security. *International Journal of Computer Science and Security*, 1(1), 2009.

[15] K. Sanzgiri, D. LaFlamme, B. Dahill, B.N. Levine, C. Shields, and E.M. Belding-Royer. Authenticated Routing for Ad Hoc Networks. *Selected Areas in Communications, IEEE Journal*, 23(3):598–610, 2005.

[16] Adrian Perrig Yih-Chun Hu and David B. Johnson. Ariadne:a secure on-demand routing protocol for ad hoc networks. *Wireless Networks*, 11(1-2):21–38, 2005.

[17] Yih-Chun Hu, David B Johnson, and Adrian Perrig. Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad Hoc Networks*, 1(1):175–192, 2003.

[18] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E.M. Belding-Royer. A secure routing protocol for ad hoc networks. In *Network Protocols, 2002. Proceedings. 10th IEEE International Conference on*, pages 78–87, 2002.

[19] Hamed Jalali Qomi and Mohammad Hesam Tadayon. Securing routing protocols against active attacks in mobile ad hoc networks. *International Journal of Computer Technology and Applications*, 2(5):1667–1673, 2011.

[20] Manel Guerrero Zapata. Secure ad hoc on-demand distance vector routing. *ACM SIGMOBILE Mobile Computing and Communications Review*, 6(3):106–107, 2002.

[21] Seung Yi, Prasad Naldurg, and Robin Kravets. Security-aware ad hoc routing for wireless networks. In *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, pages 299–302. ACM, 2001.

[22] Panagiotis Papadimitratos and Zygmunt J Haas. Secure link state routing for mobile ad hoc networks. In *Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on*, pages 379–383. IEEE, 2003.

[23] Ranga Ramanujan, Atiq Ahamad, Jordan Bonney, Ryan Hagelstrom, and Ken Thurber. Techniques for intrusion-resistant ad hoc routing algorithms (tiara). In *MILCOM 2000. 21st Century Military Communications Conference Proceedings*, volume 2, pages 660–664. IEEE, 2000.

[24] Srdjan Čapkun and Jean-Pierre Hubaux. Biss: building secure routing out of an incomplete set of security associations. In *Proceedings of the 2nd ACM workshop on Wireless security*, pages 21–29. ACM, 2003.

[25] Frank Kargl, Alfred Geis, Stefan Schlott, and Michael Weber. Secure dynamic source routing. In *System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on*, pages 320c–320c. IEEE, 2005.

[26] Baruch Awerbuch, David Holmer, Cristina Nita-Rotaru, and Herbert Rubens. An on-demand secure routing protocol resilient to byzantine failures. In *Proceedings of the 1st ACM workshop on Wireless security*, pages 21–30. ACM, 2002.

[27] Kulasekaran A Sivakumar and Mahalingam Ramkumar. An efficient secure route discovery protocol for dsr. In *Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE*, pages 458–463. IEEE, 2007.

[28] Phung Huu Phu, Myeongjae Yi, and Myung-Kyun Kim. Securing aodv routing protocol in mobile ad-hoc networks. In *Active and Programmable Networks*, pages 182–187. Springer, 2009.

[29] Pushpita Chatterjee. Trust based clustering and secure routing scheme for mobile ad hoc networks. *International Journal of Computer Networks and Communications*, 1(2), 2009.

[30] Gruia Calinescu. Computing 2-hop neighborhoods in ad hoc wireless networks. In *Ad-Hoc, Mobile, and Wireless Networks*, volume 2865 of *Lecture Notes in Computer Science*, pages 175–186. Springer Berlin Heidelberg, 2003.

[31] S.K. Bhoi, I.H. Faruk, and P.M. Khilar. Csrp: A centralized secure routing protocol for mobile ad hoc network. In *Emerging Applications of Information Technology (EAIT), 2012 Third International Conference on*, pages 429–432, 2012.

[32] Eswar Bathini and Roger Lee. Using dominating sets with 2-hop neighborhood information to improve the ad-hoc on-demand distance vector routing. In Roger Lee, editor, *Computers,Networks, Systems, and Industrial Engineering 2011*, volume 365 of *Studies in Computational Intelligence*, pages 1–9. Springer Berlin Heidelberg, 2011.

[33] P.M. John and P. Vivekanandan. A framework for secure routing in mobile ad hoc networks. In *Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on*, pages 453–458. 2012.

[34] Preeti Sachan and Pabitra Mohan Khilar. Authenticated routing for ad-hoc on-demand distance vector routing protocol. In *Advances in Network Security and Applications*, pages 364–373. Springer, 2011.